Accufacts Inc.
"Clear Knowledge in the Over Information Age"

- Pipelines -
National Security and the Public's Right-to-Know

Prepared for the
Washington City and County Pipeline Safety Consortium

by
Richard B. Kuprewicz
President, Accufacts Inc.
May 14, 2003

This report is developed from information clearly in the public domain. All observations and comments are derived from data supplied from these sources.

Executive Summary

This paper presents a brief discussion of pipeline information that should be in the public domain to reassure citizens that these systems are designed, maintained and operated prudently. Pipeline failures over the past several years have seriously tested the public's confidence in critically important gas and liquid pipeline infrastructure. Meanwhile, the events related to the terrorist activities of September 11, 2001, have raised the specter of a perceived need to withhold key information about pipelines under the guise of "national security." While these security efforts may be well meaning attempts to protect the public, such approaches provide little comfort to a concerned public raising serious questions about pipeline infrastructure running through their neighborhoods and local communities. We believe the public's apprehension is justified given the pipeline industry's efforts to deregulate their industry in the past decade, coupled with the recent shift to performance-based or risk assessment pipeline management principles that can be more difficult to quantify or audit, especially under a cloak of national secrecy.

Pipeline right-to-know discussions appear to be bounded by two extremes: the position that essentially all information concerning pipelines should be in the public domain under community right-to-know principles, and the position that no information should be made publicly available in the belief that pipelines must be hidden to protect them from terrorist threats. As is usually the case, the truth lies in a position somewhere between extremes.

Given that pipelines are uniquely sited and regulated, and that they have critical influence in our energy-based economy, the public must have the right to audit and review these important systems independently. As the Western Power Grid Episode of 2000 and 2001 has demonstrated, withholding key critical oversight information from the public can prove disastrous to citizens as well as to the security of this country.[1] A tenet in the energy industry has been repeatedly demonstrated over the past 100 years: "He who controls the pipelines controls the price." Masking or removing independent auditing of these critical systems from public eyes, no matter how well meaning the intent, is fraught with opportunity for mischief and misdeed. Such actions can come at the expense of the economic security of this nation, and pose a much greater threat than that of terrorism. With specific conditions, we propose that the Federal Energy Regulatory Commission (FERC) approach recently promulgated under new rules serve as a role model for dissemination of information. We believe this approach deals with the processes and pipeline information that should be made available to the public to assist in restoring confidence in this critically important infrastructure.

[1] FERC Report, "Final Report On Price Manipulation In Western Markets, Fact-Finding Investigation of Potential Manipulation of Electric and Natural Gas Prices," Docket No. PA02-2-000, March 26, 2003, page ES-1. "Staff concludes that large-volume, rapid fire trading by a single company, in what was incorrectly assumed to be a liquid market, substantially increased natural gas prices in California."

Pipeline Infrastructure Differs from Other Critical Infrastructure

In today's era of heightened anxiety, it is easy to jump to the wrong conclusion that most pipelines are high-priority terrorist targets. By "pipeline infrastructure," we mean all liquid and gas transmission and distribution pipeline systems. Some people believe that pipeline control centers are potential terrorist targets and that should a pipeline be attacked it would cause devastating damage to the environment and economy. Fortunately, for various reasons, the vast majority of pipeline infrastructure in this country is not a legitimate terrorist concern. This is not to say that there aren't "at-risk" terrorist sensitive pipelines, but such pipelines or pipeline segments, are very few in number and in miles.

Pipeline Control Centers are mostly mythical terrorist targets. It is easy to conclude erroneously that pipeline control centers are like other, more sensitive infrastructure control centers. Many prudent pipeline operators, however, design their systems so that their pipeline control centers cannot place these simple systems in an unsafe condition. For example, operators may design their pipeline system to be "failsafe."[2] This is not necessarily the case with much more complex facilities such as nuclear plants where control center mis-operation can have serious long-term ramifications to the public. There may be legitimate business reasons to properly secure pipeline control centers, but terrorist threat should not be the driving concern.

Reliance of gas-fired turbine electric power plants on natural gas pipelines is overstated. Many of the new power plants recently installed or planned in the U.S. are natural gas-fired turbine power plants. Some have claimed that terrorists can knock out these gas turbine power plants by attacking critical natural gas transmission pipelines feeding these facilities. It is common and prudent risk management practice for large gas turbine power plants to be installed with backup fuel supply systems. These backup systems permit continued operation of the power plant should a strategic gas supply pipeline be inadvertently lost for any reason. This duality, or independence of fuel supply, significantly reduces the often-overstated critical link between gas pipelines and such power plants, downplaying the impact of a terrorist attack on a gas pipeline.

Pipelines are quickly returned to service after an attack. In many third world countries containing limited infrastructure targets, terrorists have attacked pipelines. Even these damaged pipeline facilities, however, were quickly returned to service. This ability to rapidly return to service, known as "recovery," illustrates just one factor that differentiates pipelines from other, more highly terrorist sensitive critical infrastructure, such as nuclear or LNG/LPG[3] facilities, refineries, or chemical plants. It is very difficult to disable a prudently designed, maintained, and operated pipeline for an extended period of time. We must stress that this does not mean that a pipeline operator should not take rational steps to minimize

[2] For this paper, failsafe is defined as the installation of field equipment that prevents the control room operator from exceeding design conditions (e.g., exceeding 110% MOP/MAOP in any segment of a pipeline).

[3] LNG means liquefied natural gas (predominately methane), and LPG means liquefied petroleum gas (predominately propane and/or butane, or their mixtures).

threats. Security is just one issue in a sea of many risk concerns that a careful pipeline operator must address to insure an efficient and profitable business enterprise.

The key issue, then, is how to protect those few critical at-risk pipelines, or more specifically, pipeline segments, while providing the public reasonable access to information about the vast majority of pipelines that aren't in the security concern playing field.

General Pipeline Information Should Be in the Public Domain

When confronted with the argument that location information on a critical pipeline running through his city could not be disclosed due to national security, a city official stated, "Trying to hide that pipeline in this city is like trying to hide the Golden Gate Bridge." (Needless to say, the city official was able to get requested pipeline information after a call to his Congressman.) One can imagine the emotions of local citizens who clearly know about a nearby pipeline, but are told that information about that pipeline cannot be discussed because "locals" might be terrorists.

General information about pipelines should be made available to the public. We recommend that pipeline approximate location, size (or diameter), material shipped, and pressure be available as a matter of public record. In addition, all the historical information related to a specific pipeline's past operation should be in the public domain. Historical information includes U.S. Department of Transportation, Office of Pipeline Safety (OPS) inspection, accident and safety related condition reports, Notice of Probable Violations (or similar official correspondence), and any National Transportation Safety Board (NTSB) reports related to the investigation of major incidents.

We highly recommend that pipeline overpressure reporting exclusions in current Federal pipeline regulations be removed and regulations modified to require reporting of all overpressure events in excess of 110% Maximum Operating Pressure/Maximum Allowable Operating Pressure (MOP/MAOP) regardless of cause.[4] This historical information serves the public's interest in helping to identify serious management breakdowns, possibly suggesting a more acute problem with a specific pipeline design, operation or maintenance practice. These breakdowns can place the pipeline operator and the public at a much greater risk of harm than terrorism.

Information readily available from other sources should remain available to the public. We believe that any pipeline information that has been in the public record or that can be obtained easily is a likely candidate for remaining in the public domain. This is especially true for information that can be obtained easily outside of this country. For example, gas and liquid transmission pipeline location maps have been readily available from countless

[4] 49 CFR 195.406(b) and 49 CFR 192.201 require pipeline operators to prevent pressures from exceeding 110% MOP/MAOP anywhere in their pipeline, but other sections of Federal regulations (49 CFR 195.55(b) for liquids & 49 CFR 191.23(b) for gas) permit operators to avoid reporting such mis-operation, a serious shortcoming that flaws risk management decisions derived from the Office of Pipeline Safety database.

sources for many years. To assume that such information can be made to disappear by access restriction is unwise and foolish, and will raise serious questions as to the real reasons for keeping such information secret. Keeping obvious information from citizens is not a wise way to quell anxiety about pipelines. This tactic does little to reestablish the industry's credibility when these systems later catastrophically fail for reasons having nothing to do with terrorist activities.

Public reports of pipeline failures have significant value as "lessons learned" teaching tools providing valuable insight within the industry, the government, and the public and therefore should not be kept from the public. A key point needs to be emphasized regarding catastrophic pipeline failures. While there have been several very dramatic failures recently that underscore the tremendous energy of the materials transported in pipelines, very seldom are such tragedies a result of only one failure mechanism. Such "high profile" events are usually a consequence of a series of very serious breakdowns, which if missed or ignored long enough, inadvertently become linked and result in an extensive release of product with very high energy potential. NTSB investigations decipher unusual and dramatic pipeline failures that by their nature are not typical of many pipeline operations. These discovered failures usually identify problems of the specific pipeline operator, and are expected to be resolved either immediately before or closely following issuance of a report, and thus are not a realistic terrorist concern. The independent open report investigation process illustrated by NTSB investigations reveals major breakdowns or shortcomings in both the pipeline industry and the regulatory arena which serve the public good by expanding the general body of knowledge surrounding pipeline safety.

Risk Assessment Requires More Community Right-to-Know

Historically, pipeline inspections have relied on an inspection process, referred to as "prescriptive-based" inspection, which required inspectors to compare pipelines against a checklist of specific minimum requirements defined in Federal regulations. This "one size fits all approach" has been argued by industry as inappropriate and costly. As a result, "performance-based," or "risk assessment," is being developed and promulgated as a more effective method of assessing pipelines by government and industry. Performance-based assessment is more difficult to quantify and audit. It can be a severe problem if decision makers lack sufficient experience to understand properly various linkages that can substantially increase the likelihood and consequences (the risk) of their decisions. Risk assessment can also seriously impact various critical decisions related to the effectiveness of pipeline integrity management.

Despite its drawbacks we support the industry shift to "performance-based" pipeline management provided measurable and auditable metrics are properly defined and communicated to the public. A shift to performance-based assessments requires that specific management processes be in place to insure that risk decisions are rational and prudent. This process relies on identifying specific risks of concern and presenting methods that appropriately address them. A review of the Bellingham Safety Immediate Action Plan illustrates key concepts of such a performance-based approach that go beyond integrity

management concerning pipeline operation in a highly sensitive area.[5] With this approach, specific risks of concern are identified, via objective headings for most sections, and then various actions to address these objectives are further defined. Please note that these specifically defined requirements should not be universally or blindly applied to other segments of Olympic Pipeline's system, nor to other gas or liquid pipelines. "Risks of concern" will be different for various pipelines and pipeline segments.

While we applaud the OPS for developing and pursuing improvements in pipeline integrity management approaches for high consequence areas, we must clarify two points concerning public or community right-to-know issues involving integrity management. As mentioned earlier, communities want assurances that real risks of concern are under control by a prudent pipeline management team. Pipeline operators should be able to list or identify those risks of concern for a particular pipeline segment and share this information with the public. Secondly, pipeline operators should be able to engage the community in a discussion of the technologies the company is utilizing to identify and rank the types of anomalies characteristic of these identified risks. For example, if external corrosion has been recognized as a specific threat in a city, the use of a particular smart pig (an in-line inspection tool) may be an appropriate identified tool to be discussed in a public forum. The identification of specific anomaly locations is of little value to the public unless the pipeline operator has exhibited poor management processes that could result in unwise risk management decisions. Such a situation would clearly warrant a more detailed release of information to the public. It is a myth that identification of anomaly general locations or type indicates weaknesses in pipelines that terrorist may cultivate.

For Specific Pipeline Technical Information Follow the FERC Roadmap with Four Conditions

Certain types of detailed technical information do not need to be in the public domain. While some may claim a need for such detailed information about pipelines, seldom is such a volume of pipeline information needed to ascertain serious problems in pipeline management, operations, design, construction or maintenance. In fact, we consistently find that too much information tends to inhibit pipeline operators from evaluating and operating their systems prudently. In reaching a proper balance of too little or too much information, we have scrutinized the approach developed as a final rule by FERC pertaining to critical energy infrastructure information ("CEII")[6] and believe this model has merit provided the conditions listed below are followed.

The new FERC rule requires a pipeline company to provide approximate location information, but limits the free flow (restricted access via the internet, but available in certain

[5] Bellingham Safety Immediate Action Plan issued September 7, 1999, and signed September 10, 1999, developed jointly between the City of Bellingham and Olympic Pipeline following the Olympic Pipeline failure of June 10, 1999, in Bellingham, WA. The Action Plan is available at public web site: http://www.cob.org/pipeline/safetyplan.htm.

[6] FERC "Critical Energy Infrastructure Information," Docket Nos. RM02-4-000, DL 02-1-000, Order No. 630, issued February 21, 2003.

record rooms) of general public information, and prevents the release of detailed information related to specific equipment that might be considered helpful to terrorists.[7] Examples of publicly available information include: topographical maps, alignment sheets, site project boundaries and general location maps. Detailed restricted information (captured under the CEII label) includes Process and Instrument Diagrams (P&ID's), flow diagrams showing volumes and pressures, LNG facilities, and drawings indicating specific building labels (i.e., control room or compressor building). The pipeline operator makes the declaration as to which pipeline information is CEII. Note that CEII labeled or protected information may still be made available via the Freedom of Information Act (FOIA) or through application to a newly defined FERC position, the CEII Coordinator. The CEII Coordinator is responsible for determining what information qualifies as CEII and processing requests for CEII. Although there are FERC and judicial appeal processes, the burden falls on requestors to prove that declared CEII should be made available for review.

We support FERC's new approach as a model with the following conditions:

1) **This approach does not become a hindrance to the various intervener processes**. Intervention processes, whether FERC, state, or local, require and assume the timely exchange of appropriate information. Such processes provide an important check and balance in verifying "public convenience and necessity" tests of pipeline infrastructure. It is the finding of public convenience and necessity that usually gives various federal and state agencies condemnation power when siting pipelines. Newly implemented FERC expedited/centralized approval processes raise serious issues about the ability to provide timely and thorough review of pipelines given CEII restrictions. The new steps to uncover key restricted CEII information places additional time and resource burdens on the public.

2) **Declaration of critical information as CEII is not abusively applied**. The broad definition of CEII could be easily misinterpreted to apply to all pipeline equipment, which could circumvent the flow of appropriate and timely information to stakeholders. Although FERC has clearly indicated that this is not the intent and has warned companies against such abusive tactics, given the apparent light penalties for such abuse and weak FERC enforcement options, serious concern remains that labeling critical information as CEII could be applied abusively.

3) **CEII characterization is not used as a shield to prevent disclosure of information needed to participate in civil or criminal pipeline litigation or other legal actions**. The CEII characterization could be invoked by a party as a means of preventing disclosure of important information in a lawsuit or other legal proceeding. Such prevention could undermine the discovery process and detrimentally affect the legal proceeding. Judicial avenues already in place permit appropriate discovery while restricting public release of sensitive data.

[7] IBID, pages 19 – 26.

4) **National security information restrictions do not prevent access to certain sensitive information required for independent review of pipelines**. Federal and state pipeline safety agencies, emergency responder agencies, local governments, and "access professionals" responsible for providing independent review of such pipelines by these agencies or stakeholders need to have access to CEII in order to perform their duties. This is an important safety valve to insure national security claims are not abused, as day-to-day pipeline safety operations play a vital role in national security as well.

While not yet tested, the new FERC approach, with the above-identified conditions, appears to be a rational model that should be applied to the dissemination of all pipeline information. This model should be valid for all new or existing pipeline facilities, including those pipelines not under FERC jurisdiction.